Department of Defense Endpoint Security

Remote Workforce Interim Security Brief

March 18th 2020

McAfee™

The Current Problem

1. COVID-19 caused a huge increase of work from home users with no VPN capacity

2. Remote work rapidly increased the amount of traffic outside of managed DoDIN

3. How can we quickly increase security posture for these devices?

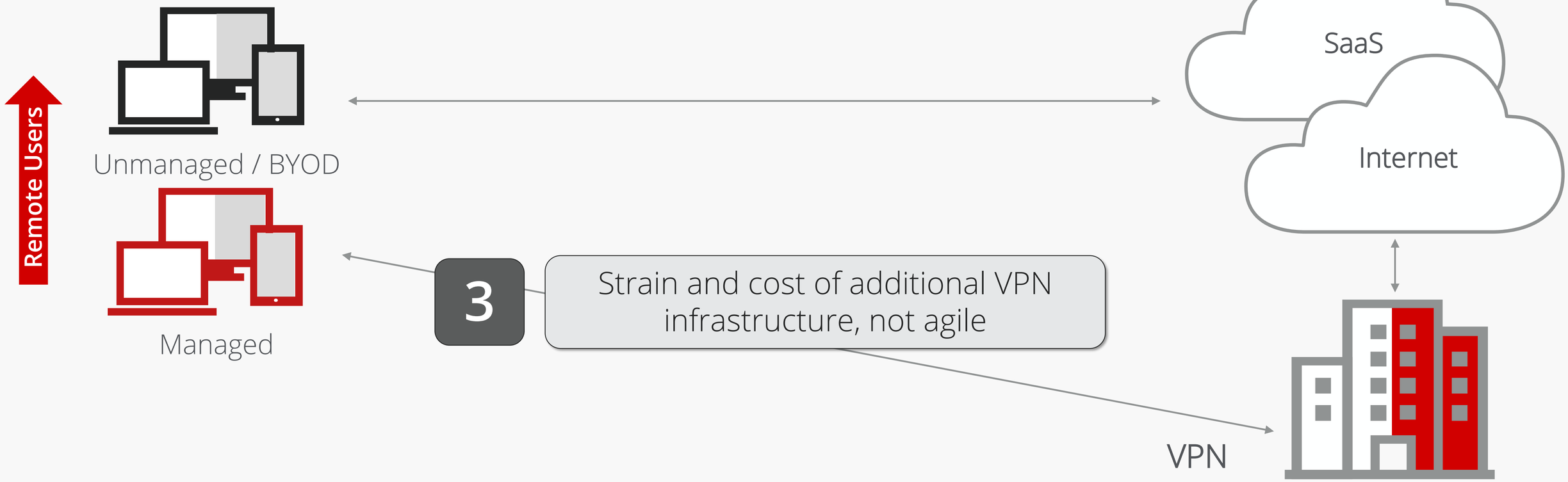
Remote Work Challenges

- Current existing VPN Infrastructure does not scale quickly for new load of remote workers.
- Remote managed users are unable to update security content on DoD devices without VPN connections.
- How do we protect our users and our data while granting them access to web resources without VPN access?
- Remote Users have varying degree of Managed and Unmanaged assets, how can we add protection to unmanaged devices?

Security Implications

1 Vulnerable DoD devices for lack of security updates

2 Major increase of DoD devices not on VPN vulnerable to unsafe web browsing



3 Strain and cost of additional VPN infrastructure, not agile

Explosion of Work from Home

Interim Solution – Easy Deployment

Provide security content updates, enable secure Internet access, and secure personal devices

1. **Security Updates from McAfee –** Policy change in ePO to provide the ability to install daily security updates for VSE (DAT) and ENS (AMCore) direct from McAfee.

2. **Protect Personal Devices –** McAfee Total Protection DoD home use subscription provided to protect personal PCs, MACs, smartphones, and/or tablets.

3. **Secure Internet Access for non-VPN users –** Secure browsing for remote users via McAfee UCE-B Web Gateway Cloud Service (WGCS) by providing SSL Inspection, URL Blocking, and Malware detection mapped to current web proxy policies.

Security Updates Direct from McAfee

Ensure managed VSE & ENS endpoints have current malware definitions (DAT and AMCore) on or off the VPN

McAfee assumes the ESS Administrator will translate these instructions as appropriate for each unique environment to avoid mission impact

Procedure

1. Duplicate existing McAfee Agent (MA) General policy in ePO and rename. From the **Update** tab, select only:
   - *AMCore Content Package, DAT (if applicable), and Buffer Overflow DAT for VSE (if applicable)*

2. Duplicate existing MA Repository Policy in ePO and rename. From the **Repositories** tab, add a new repository with the following settings:
   - *HTTP Repository*
   - DNS Name: *update.nai.com/products/commonupdater3/*
   - Port: *80*

3. Duplicate HIPS Firewall Policy and rename. Add the following rule:
   - Name: *McAfee Commercial*
   - Action: *Allow*
   - Direction: *Either*
   - Remote Network using FQDN: *update.nai.com*
   - Leave remaining options default

4. Assign modified policies to **pilot group** and validate endpoints can perform an "Update Security" successfully off the VPN
5. Push new interim policies in phases once changes have been fully vetted and tested

Protect Personal Devices

McAfee Internet Security is a consumer solution providing comprehensive protection for personal PCs and MACs through McAfee's DoD Home Use Program. This program includes 24/7 McAfee Consumer Support for all employees participating in the program.

Procedure

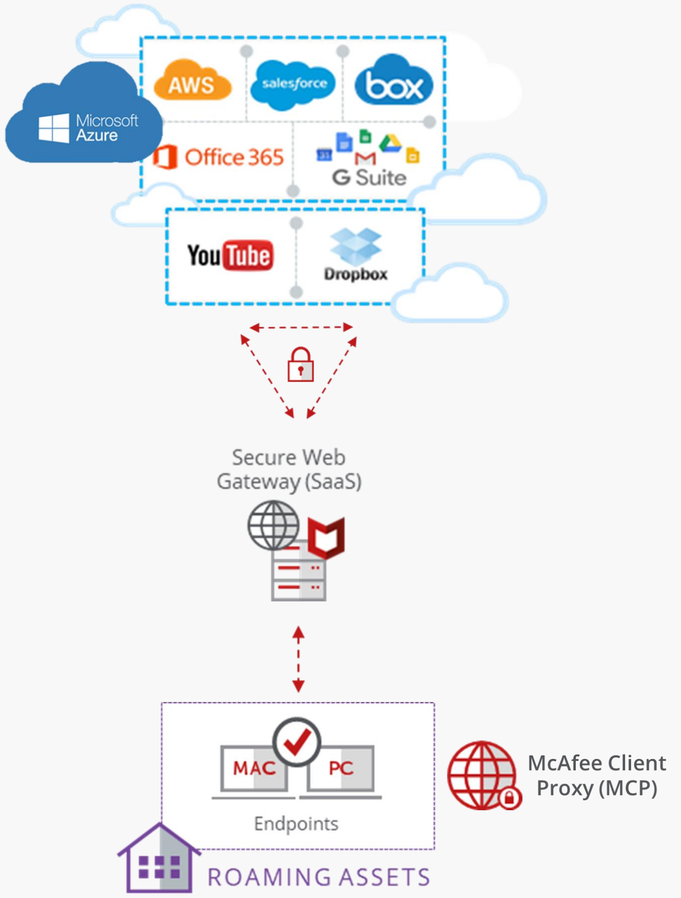
1. Navigate to the DISA Antivirus for Home Use website: https://www.disa.mil/Cybersecurity/Network-Defense/Antivirus/Home-Use.
2. Follow the instructions to receive your product code and links to the download
   - *Updates to the internal page are forthcoming*

McAfee Internet Security is for personal devices only; do not install on Government Furnished Equipment (GFE)

Secure Internet Access – with No VPN

Utilize the DoD McAfee Client Proxy (MCP) on managed endpoints to redirect web traffic through McAfee's UCE-B WGCS SaaS solution where existing web proxy policies are applied and enforced

McAfee assumes the ESS Administrator and Web Proxy Administrator will translate these instructions as appropriate for each unique environment to avoid mission impact
This option is an additional cost and is licensed as a subscription per user.



Procedure

1. Install and Configure McAfee WebGateway Virtual instance
2. Duplicate Existing Proxy SSL, URL Filtering, and Anti-Malware rules into McAfee WebGateway
3. Configure Web Hybrid
4. Sync WebGateway policy with WebGateway Cloud Service
5. Configure MCP Policy via McAfee MVision ePO
   - Export MCP Policy from MVision ePO and Import to on-premises ePO
6. Deploy MCP agent to **pilot group**
7. Assign modified policies to **pilot group** and validate endpoints can access predetermined website successfully off the VPN
8. Push new MCP agent and new interim policies in phases once changes have been fully vetted and tested

Other Solutions of Interest

Office 365 Protection

Total control over data and user activity in O365 through McAfee MVISION Cloud CASB

Key Features

- Prevent sensitive data that cannot be stored in the cloud from being uploaded to or created in Office 365
- Prevent sharing of sensitive or regulated data in Office 365 with unauthorized parties in real-time
- Detect threats from compromised accounts, insider threats, privileged access misuse, and malware infection
- Capture a complete audit trail of all user activity enriched with threat intelligence to facilitate post-incident forensic investigations

Mobile Device Security

Detect threats and vulnerabilities on iOS & Android devices, connected networks, and downloaded apps through McAfee MVISION Mobile

Key Features

- On-device, real-time protection that detects mobile threats and protects against zero-day attacks through machine learning capabilities
- Enterprise-grade actionable mobile threat intelligence to help you better understand and quickly respond to mobile threats
- Compliance controls for mobile devices, allowing your employees to work anywhere, any time, and on any device
- Protect users against phishing by detecting harmful links found in text messages, social media apps, and emails

Thank you.